REMARKS/ARGUMENTS

Claim Amendments

The Applicant has amended claims 8 and 11 and new claim 15 has been added. The amendments were made to define an acronym in claim 8 and to clarify the language of claim 11. Applicant respectfully submits no new matter has been added. Accordingly, claims 8-15 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

Claim Rejections – 35 U.S.C. § 103 (a)

Claims 8-14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Ylonen et al (US 6,438,612 B1) and further in view of Nikander, et al. (US 6,253,321 B1). The Applicant respectfully traverses the rejection of these claims.

The Ylonen reference is cited for disclosing a plurality of security procedure modules coupled to the IPFWs (Figures 6 and 7, Col. 8 lines 46-66). A portion of Ylonen disclosing virtual routers each having its own IPSEC processor is cited in support of the assertion (Figures 6 and 7). However, Applicant has reviewed this cited portion of Ylonen and finds no reference to a security controller, as in the Applicant's invention, that allocates negotiated SAs among Security Procedure modules and notifies both the IPFWs and the security procedure modules. Though the argument cites three alternative architectures as disclosed in Ylonen, none of the architectures cite the use of security procedure modules. The three alternatives describe three different uses of the SAs or SPIs.

Applicant's claim 8 combination recites the use of a security controller to allocate negotiated SAs among particular security procedure modules. The plurality of security modules is coupled to at least one IP forwarder that receives IP packets and determines and forwards a packet to the IP packet destination. A security controller (SC) module is disclosed for distributing IPSec policies to a plurality of Security Procedure (SecProc) modules. When new SAs are created the SC determines which SecProc modules are appropriate for placing the new SAs, and the IPFW sends the IP packets to the security

module implementing the associated SA. Included in the Applicant's IPSec architecture are three components: an IP forwarder for determining the destination of the packets, a plurality of security procedure modules for receiving the IP packets and a security controller (SC) for allocating negotiated SAs among the modules. The SC also notifies the security procedure modules and the IP forwarder of the allocation.

The present invention discloses that the Applicant's IPSec architecture is comprised of components that include a plurality of security procedure modules and this is not the same as that disclosed by Ylonen. The Applicant discloses Security Procedure modules as integral to the invention and the "...main modules in IPSec packet handling." (para [0061]). The portion of Ylonen cited as disclosing a plurality of security procedure modules actually discloses multiple IPSEC engines while the present invention discloses an IPSec engine comprising multiple Security Procedure modules.

Paragraph 3(a)(i)(3) of the Detailed Action indicates that the automatic key manager block and an IPSEC block communicate with a security policy database and apply the IKE protocol for setting up the security association. Paragraph 3(a)(i)(3)(ii) indicates that Ylonen is silent on the capability of a security controller but also appears to equate a security controller to the IPSec engine, i.e., "...a security controller (i.e., IPSEC engine)".

The Nikander reference is cited for disclosing a security controller. The security controller of Nikander, though not specifically identified as a security controller, appears to be "a separate policy manager that makes the actual policy decisions..." (Col. 4, lines45-48). The policy manager makes actual policy decisions and generates new compiled filter code and implements policy (Col. 4, 45-53).

The Applicant's controller in contrast to the policy manager of Nikander distributes IPSec policies to Security Procedure modules and when new security associations are created the Security Controller determines the Security Procedure modules that are to receive the new SAs. The Security Procedure modules, "...execute(s) IPSec encryption, decryption and authentication" (para. [0062]).

It is respectfully submitted that Nikander does not address Ylonen's lack of a plurality of Security Procedure modules with respect to Applicant's invention. The combination of the Ylonen and Nikander references fails to teach utilizing a security controller that allocates negotiated SAs among a plurality of security procedure modules. The Applicant respectfully requests the withdrawal of the rejection of claim 8. Claims 9-13 depend from claim 8 and contain the same novel limitations. This being the case, the Applicant respectfully requests the withdrawal of the rejection of claims 9-13. Additionally, claim 14 is analogous to and contains limitations similar to those in independent claim 8. The withdrawal of the rejection of claim 14 is also respectfully requested.

Claims 9-11 are rejected as having limitations similar to those of claim 12. The Applicant respectfully traverses the rejection of these claims.

Coupling security procedure modules together for forwarding an IP packet from one security procedure module to another of the plurality of modules is the limitation disclosed in claim 9. Respectfully, claim 9 discloses coupled security procedure modules, claims 10 and 11 disclose modifying IP packet filters, which are responsible for routing IP packets to the security procedure modules and the SPI is one of the selectors for filtering the packets. Claim 12 discloses the coupling of an IKE module to the security controller and the interaction between the security controller and the IKE module. Thus, claims 9-11 do not have similar limitations to those limitations in claim 12. In fact, claim 12 depends directly from claim 8 as do claims 9 and10 (claim 11 depends from claim 10) and contains the limitations of claim 8, but not the limitations of claims 9-11. Therefore, the Applicant respectfully requests the withdrawal of the rejection of claims 9-11.

Claims 12 and 13 each depend directly from claim 8 and contain the limitation of a plurality of security procedure modules which the Ylonen and Nikander both lack and the Applicant respectfully requests the withdrawal of the rejection of claims 12 and 13.

Prior Art Not Relied Upon

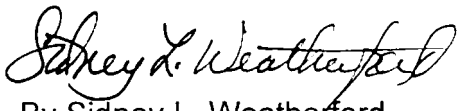
In paragraph 5 on page 6 of the Office Action, the Examiner stated that the prior art made of record and not relied upon is considered pertinent to the Applicant's disclosure.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,



By Sidney L. Weatherford
Registration No. 45,602

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-8656
sidney.weatherford@ericsson.com